

#6 Priority Doc.
M. Bruggen
8/31/01
PCT/US

99/21663

日本国特許庁
PATENT OFFICE
JAPANESE GOVERNMENT

REC'D 26 OCT 1999

WIPO PCT

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application:

1998年 9月29日

出願番号
Application Number:

平成10年特許願第275513号

出願人
Applicant(s):

株式会社エーエスエー・システムズ
河口 英二
リチャード オー イースン

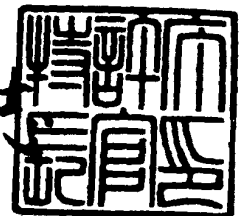
PRIORITY
DOCUMENT

SUBMITTED OR TRANSMITTED IN
COMPLIANCE WITH RULE 17.1(a) OR (b)

1999年 5月28日

特許庁長官
Commissioner,
Patent Office

伴佐山 建志



出証番号 出証特平11-3033763

【書類名】 特許願

【整理番号】 98X072

【提出日】 平成10年 9月29日

【あて先】 特許庁長官 殿

【国際特許分類】 G06K 17/00

【発明の名称】 情報カードおよび情報カードシステム

【請求項の数】 12

【発明者】

【住所又は居所】 福岡県宗像市日の里8丁目21番地の2

【氏名】 河口 英二

【発明者】

【住所又は居所】 アメリカ合衆国 04473 メイン州 オロノ市 アールアール5 ボックス240ケイ

【氏名】 リチャード オー イースン

【発明者】

【住所又は居所】 福岡県北九州市戸畑区中原新町3-3 株式会社エーエスエー・システムズ内

【氏名】 津田 邦博

【特許出願人】

【住所又は居所】 福岡県北九州市戸畑区中原新町3-3

【氏名又は名称】 株式会社エーエスエー・システムズ

【代表者】 麻上 俊泰

【特許出願人】

【住所又は居所】 福岡県宗像市日の里8丁目21番地の2

【氏名又は名称】 河口 英二

【特許出願人】

【住所又は居所】 アメリカ合衆国 04473 メイン州 オロノ市 アールアール5 ボックス240ケイ

【氏名又は名称】 リチャード オー イースン

【代理人】

【識別番号】 100094215

【弁理士】

【氏名又は名称】 安倍 逸郎

【電話番号】 093-533-9451

【手数料の表示】

【予納台帳番号】 037833

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 情報カードおよび情報カードシステム

【特許請求の範囲】

【請求項 1】 画像データまたは音響データからなる情報データを格納する記憶部を備えた情報カードにおいて、

上記情報データにステガノグラフィによる固有データを埋め込んだ情報カード

。

【請求項 2】 上記固有データは、情報カードの正当性、または、情報カードの所有者を示すものである請求項 1 に記載の情報カード。

【請求項 3】 上記記憶部には、上記情報データの読み出しを許可するためのパスワードが格納された請求項 1 または請求項 2 に記載の情報カード。

【請求項 4】 上記情報カードでは、上記情報データから固有データを抽出する許可を与えるためにカスタマイズキーが用いられる請求項 1 ～請求項 3 のいずれか 1 項に記載の情報カード。

【請求項 5】 画像データまたは音響データからなる情報データを格納する記憶部を備え、この情報データにステガノグラフィによる固有データを埋め込むとともに、上記情報データの読み出しを許可するためのパスワードが上記記憶部に格納された情報カードと、

パスワードを入力するための入力手段、入力されたパスワードを上記情報カードに格納したパスワードと照合することにより上記情報データの読み出しを許可するパスワード照合手段、読み出された情報データを出力する出力手段を有するデータ処理端末とを備えた情報カードシステム。

【請求項 6】 画像データまたは音響データからなる情報データを格納する記憶部を備え、この情報データにステガノグラフィによる固有データが埋め込まれた情報カードと、

カスタマイズキーを入力するための入力手段、入力されたカスタマイズキーを用いて上記固有データを抽出する固有データ抽出手段、抽出された固有データを出力する出力手段を有するデータ処理端末とを備えた情報カードシステム。

【請求項 7】 上記情報カードの記憶部に、上記情報データの読み出しを許

可するためのパスワードを格納するとともに、

上記データ処理端末は、パスワードを入力するための入力手段と、入力されたパスワードを上記情報カードに格納したパスワードと照合することにより上記情報データの読み出しを許可するパスワード照合手段と、読み出された情報データを出力する出力手段とを有する請求項 6 に記載の情報カードシステム。

【請求項 8】 上記抽出された固有データは、ホストから読み込まれたまたは外部から入力された固有データとその全部または一部が照合される請求項 5 ～請求項 7 のいずれか 1 項に記載の情報カードシステム。

【請求項 9】 ステガノグラフィによる固有データの埋め込みは、情報データとして作成した画像データまたは音響データを自然 2 進コードとし、または、自然 2 進コードから正準グレイコード表現に変換し、この自然 2 進コードまたは正準グレイコードをビットプレーン分解するとともに、このビットプレーン上を複雑さの尺度で領域分割し、この複雑な部分を構成するデータと上記固有データとを置換する請求項 1 ～請求項 8 のいずれか 1 項に記載の情報カードまたは情報カードシステム。

【請求項 10】 上記埋め込み用の固有データにコンジューゲーション演算を施した請求項 9 に記載の情報カードまたは情報カードシステム。

【請求項 11】 上記情報カードの記憶部は IC チップで構成された請求項 1 ～請求項 10 のいずれか 1 項に記載の情報カードまたは情報カードシステム。

【請求項 12】 上記情報カードにはその本体表面に写真が搭載されているとともに、上記情報データまたは固有データはその写真を示す画像データである請求項 1 ～請求項 11 のいずれか 1 項に記載の情報カードまたは情報カードシステム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

この発明は情報カードおよび情報カードシステム、詳しくはステガノグラフィ (Steganography ; 画像深層暗号化方法、電子的あぶりだし技法、

情報非可視化技法、またはデジタル封筒技法）を用いたクレジットカード、キャッシュカード、IDカードなどとして利用される情報カードおよびこの情報カードを用いた情報カードシステムに関する。

【0002】

【従来の技術】

従来のこの種の情報カードとしては、例えばクレジットカード、IDカードなどとして使用されるICカードが知られている。

このICカードは、プラスチック板にICチップを埋め込んだものであり、このICチップには、マイクロプロセッサとメモリまたはメモリのみが搭載されている。前者がいわゆるICカードであって、後者がメモリカードと称される。

そして、このICカードをクレジットカードとして使用する場合、プラスチック板表面にはそのカード所有者名、カード番号が表示され、ICチップのメモリ（ROM）には認証プログラムや暗証番号などが格納されていた。さらに、これらの認証プログラムやこれに使用する暗証番号などは、不法なアクセスから保護するため、暗号文で記載されることもあった。

【0003】

【発明が解決しようとする課題】

しかしながら、このような従来のICカードにあっては、そのセキュリティが十分ではなかった。すなわち、暗証番号の不正入手により、また、暗号文の解読により、当該ICカードが不正使用されることがあった。または、ICカード自体が偽造されることがあった。そして、このような偽造カードであっても暗証番号を入手することができれば、その使用を防ぐことができなかった。

【0004】

【発明の目的】

そこで、この発明は、カードの偽造を完全に防止することができる情報カードおよび情報カードシステムを提供することを、その目的としている。

また、この発明の目的は、カードの不正使用を完全に防止することができる情報カードおよび情報カードシステムを提供することにある。

【0005】

【課題を解決するための手段】

請求項 1 に記載の発明は、画像データまたは音響データからなる情報データを格納する記憶部を備えた情報カードにおいて、上記情報データにステガノグラフィによる固有データを埋め込んだ情報カードである。この情報カードは、物理的形態としては例えば IC カード、光カードなどに適用することができる。

【0006】

請求項 2 に記載の発明は、上記固有データは、情報カードの正当性、または、情報カードの所有者を示すものである請求項 1 に記載の情報カードである。

【0007】

請求項 3 に記載の発明は、上記記憶部には、上記情報データの読み出しを許可するためのパスワードが格納された請求項 1 または請求項 2 に記載の情報カード

【0008】

請求項 4 に記載の発明は、上記情報カードでは、上記情報データから固有データを抽出する許可を与えるためにカスタマイズキーが用いられる請求項 1 ～請求項 3 のいずれか 1 項に記載の情報カードである。このカスタマイズキーとは、埋込プログラム（エンコーダプログラム）または取り出しプログラム（デコーダプログラム）の流れを制御するデータである。カスタマイズキーは情報カードの正当使用権限者のみが知ることができるものとすることができる。

【0009】

請求項 5 に記載の発明は、画像データまたは音響データからなる情報データを格納する記憶部を備え、この情報データにステガノグラフィによる固有データを埋め込むとともに、上記情報データの読み出しを許可するためのパスワードが上記記憶部に格納された情報カードと、パスワードを入力するための入力手段、入力されたパスワードを上記情報カードに格納したパスワードと照合することにより上記情報データの読み出しを許可するパスワード照合手段、読み出された情報データを出力する出力手段を有するデータ処理端末とを備えた情報カードシステムである。データ処理端末は情報カードとの間でデータの授受が有線または無線（接触または非接触状態で）により可能とすることができる。

【0010】

請求項6に記載の発明は、画像データまたは音響データからなる情報データを格納する記憶部を備え、この情報データにステガノグラフィによる固有データが埋め込まれた情報カードと、カスタマイズキーを入力するための入力手段、入力されたカスタマイズキーを用いて上記固有データを抽出する固有データ抽出手段、抽出された固有データを出力する出力手段を有するデータ処理端末とを備えた情報カードシステムである。

【0011】

請求項7に記載の発明は、上記情報カードの記憶部に、上記情報データの読み出しを許可するためのパスワードを格納するとともに、上記データ処理端末は、パスワードを入力するための入力手段と、入力されたパスワードを上記情報カードに格納したパスワードと照合することにより上記情報データの読み出しを許可するパスワード照合手段と、読み出された情報データを出力する出力手段とを有する請求項6に記載の情報カードシステムである。

【0012】

請求項8に記載の発明は、上記抽出された固有データは、ホストから読み込まれたまたは外部から入力された固有データとその全部または一部が照合される請求項5～請求項7のいずれか1項に記載の情報カードシステムである。

【0013】

請求項9に記載の発明は、ステガノグラフィによる固有データの埋め込みは、情報データとして作成した画像データまたは音響データを自然2進コードとし、または、この自然2進コードから正準グレイコード表現に変換し、これらの自然2進コードまたは正準グレイコードをビットプレーン分解するとともに、このビットプレーン上を複雑さの尺度で領域分割し、この複雑な部分を構成するデータと上記固有データとを置換する請求項1～請求項8のいずれか1項に記載の情報カードまたは情報カードシステムである。

【0014】

請求項10に記載の発明は、上記埋め込み用の固有データにコンジュゲーション演算を施した請求項9に記載の情報カードまたは情報カードシステムである。

【0015】

請求項 11 に記載の発明は、上記情報カードの記憶部は IC チップで構成された請求項 1 ～請求項 10 のいずれか 1 項に記載の情報カードまたは情報カードシステムである。

【0016】

請求項 12 に記載の発明は、上記情報カードにはその本体表面に写真が搭載されているとともに、上記情報データまたは固有データはその写真を示す画像データである請求項 1 ～請求項 11 のいずれか 1 項に記載の情報カードまたは情報カードシステムである。

【0017】

【作用】

請求項 1 に記載の発明において、情報カードは、その記憶部に情報データを格納している。この情報データは画像データまたは音響データにより構成されている。そして、この情報データにはステガノグラフィによる固有データが埋め込まれている。

この結果、第三者がこの情報カードから情報データを読み出し得たとしても、ステガノグラフィによる固有データは情報データにより隠されているため、その固有データ（秘密情報）の存在自体を第三者に気付かせることがない。よって、情報カードとしてのセキュリティを高めることができる。なお、情報データとしては、ステガノグラフィによる固有データの埋込を可能とする程度の容量を有するものであればよい。

【0018】

請求項 2 に記載の発明においては、上記固有データは、情報カードの正当性、または、情報カードの所有者を示している。よって、この固有データを参照して情報カードの正当性（偽造、改ざんの有無）を確認、検証することが容易となる。また、これらの正当性、所有者のデータの存在を隠すことができる。

【0019】

請求項 3 に記載の発明においては、記憶部に情報データの読み出しを許可する

ためのパスワードを格納しているため、このパスワードを照合することにより、その情報データの読み出しを許可することができる。よって、そのセキュリティを高めることができる。

【0020】

請求項4に記載の発明においては、カスタマイズキーを用いることにより、情報データから固有データの抽出を可能とする。このカスタマイズキーは情報カードには格納されていないため、このカスタマイズキーが盗まれるおそれがない。よって、その安全性を高めることができる。

【0021】

請求項5に記載の発明においては、情報カードに情報データを格納し、この情報データにステガノグラフィによる固有データを埋め込んでいる。また、この情報データの読み出しを許可するためのパスワードも情報カードに格納している。そして、データ処理端末は、入力されたパスワードを情報カードに格納したパスワードと照合する。よって、パスワードが一致したとき、情報カードからの情報データの読み出しが許可され、読み出された情報データが出力される。例えばディスプレイ表示、音声出力、通信回線を介しての電子的データとしての出力である。

この結果、情報カードに格納した情報データの読み出しについては、パスワード照合により保護される。無権限者の読み出しは禁止されるからである。

【0022】

請求項6に記載の発明においては、情報カードには情報データと固有データとが保有されている。

データ処理端末では、入力されたカスタマイズキーを用いて固有データを抽出するが、正規のカスタマイズキーの場合に限り、固有データの抽出が許容される。

したがって、このシステムでは、もし固有データの埋め込みがあると考えられた場合でも、その抽出を防止することができる。第三者はカスタマイズキーを知ることができないからである。また、第三者が適当に入力することにより正規のカスタマイズキーと一致させることは不可能であるからである。よって、システ

ム自体のセキュリティが高められている。

【0023】

請求項7に記載の発明では、上記情報カードには、情報データ（固有データ）の他に上記パスワードを格納してある。データ処理端末は、パスワードにより情報データを保護し、かつ、カスタマイズキーを用いて固有データを保護する。よって、2重の意味でのプロテクションが、固有データの抽出にかけられていることとなる。

【0024】

請求項8に記載の発明においては、データ処理端末にホストから固有データを読み込むか、外部から固有データを入力する。この読み込みまたは入力された固有データの全部または一部を、情報カードに格納してある固有データのそれと照合する。そして、一致している場合、この情報カードによるプログラム処理を可能とすることができる。例えばクレジットカードとしての機能を発揮可能とする。

この結果、3重の意味でのセキュリティをこのシステムに施すことができる。よって、偽造、不正使用を完全に排除することができる。

【0025】

請求項9に記載の発明において、ステガノグラフィによる固有データの埋め込みは、まず、情報データを自然2進コードに変換し、この状態で、または、自然2進コードを正準グレイコード表現に変換する。さらに、この自然2進コードまたは正準グレイコードをビットプレーン分解する。とともに、このビットプレーン上を複雑さの尺度で領域分割し、この複雑な部分を構成するデータを作成した固有データと置換する。この結果、情報カードの記憶部には、固有データが埋め込まれた情報データが格納されることとなる。また、この固有データはその存在が秘匿される。

【0026】

請求項10に記載の発明においては、上記埋め込み用の固有データにコンジューゲーション演算を施している。その結果、各種ファイルを埋め込むことが可能である。

【0027】

請求項 11 に記載の発明においては、上記情報カードの記憶部は IC チップで構成されている。したがって、いわゆるメモ리카ードまたは IC カードとして情報カードおよびそのシステムを構成することが可能である。このように IC カードとして構成することにより、データ処理端末としてリーダライタを安価に設けることも可能となる。

【0028】

請求項 12 に記載の発明においては、上記情報カードの本体表面に写真を搭載し、かつ、上記情報データまたは固有データはその写真を示す。よって、画像データの出力表示により、それらの照合が可能となる。安全性がさらに高まることとなる。

【0029】

【発明の実施の形態】

以下、この発明に係る情報カードシステムの一実施例について説明する。

図 1 はこの発明に係るシステムの概念を示すブロック図である。すなわち、この情報カードシステムは、情報カードと、この情報カードとの間でデータの授受を行うことができるデータ処理端末と、データ処理端末との間でデータの授受を行うホストコンピュータとを備えて構成されている。情報カードは、データを記憶する記憶部を有し、この記憶部には、固有データをステガノグラフィ技術により埋め込んだ情報データ、パスワードを格納している。データ処理端末は、入力手段、出力手段、パスワード照合手段、固有データ抽出手段を有している。

したがって、この情報カードシステムによれば、データ処理端末は、パスワードの照合を行うことにより、情報データの読み出しが可能となる。また、カスタマイズキーを用いて固有データの抽出を行うことができる。よって、この情報カードをクレジットカードなどとして使用する場合、そのカード所有者以外の使用を完全に排除することができる。さらに、そのカードの偽造による不正な使用についても完全に排除することができる。

【0030】

特に、固有データは、ステガノグラフィ (BPCS-Steganograph

hy)により情報データ中に埋め込まれているため、上記偽造および無権限者による抽出を完全に排除することができる。

ここに、BPCS-Steganography (Bit-Plane Complexity Segmentation Steganography) とは、例えば画像データを各構成ビットにスライスして得られる「ビットプレーン」に関し、そのプレーン上の2値パターンの複雑さ(ランダムさ)に注目して、ランダム部分を秘密データと置き換える(埋め込む)技術である。従来から知られていたステガノグラフィでの埋め込み容量が5~10%程度であったのに比べ、BPCS-ステガノグラフィの埋め込み容量は、50%程度から場合によっては70%程度に及ぶ。画期的な大容量化を実現できるものである。

BPCS-Steganography技術は以下の4つの基本アイデアから成立している。

すなわち、(1)画像データの自然2進コード表現(PBC)として、または、自然2進コードから「正準グレイコード表現(CGC)」に変換してビットプレーン分解を行うこと。(2)ビットプレーン上を2値パターンの「複雑さの尺度」で領域分割し、複雑な部分(ランダムな部分)を秘密データと入れ替える(埋め込む)こと。このようにしても人目には全くわからない。(3)埋め込みファイルに「コンジュゲーション操作」を施し、どのような種類のファイルでも埋め込めるようにしたこと。(4)BPCS-Steganographyのアルゴリズム(符号化・復号化プログラム)をユーザ毎にカスタマイズする機能を付けたこと。このことでパスワードとは異なる「カスタマイズキー」による埋め込み情報の安全性が確立された。

BPCS-Steganography技術の最大の特徴は埋込容量が大容量であることだが、この特徴により以下の応用が可能である。

すなわち、(A)秘密を埋め込んでいることを他人に気付かれないこと。秘密を埋め込んだ画像と埋め込んでいない画像との区別が不可能であること。(B)たとえ秘密が埋め込まれていることがわかって、どこから、どのようにして秘密情報を取り出せるのかが、カスタマイズキーなしではまったく判らないこと。

【0031】

したがって、このカードシステムでは、従来型のカード（顔写真付き）に8KB以上のICメモリを搭載したステガノ・カードを使用する。このカードの運用は以下のように行う。

（1）ICメモリ中にカード所有者本人の顔写真データを記憶しておく。このデータを読み出すには、データ読み出し装置にカードのパスワードを入力しなければならない。

（2）その顔写真データには、BPCS-Steganography技術により、カード所有者の個人情報（例えば、指紋、個人の履歴、親族データ、趣味データなど）を埋め込んでおく。

（3）埋込情報を取り出し、ディスプレイに表示するためには、正しいカスタマイズキーの入力が必要である。このキー情報については、以下の通りである。

（a）一部をカード所有者だけが知っている（個人キー）。

（b）残部はカード会社だけが厳重に秘密管理しており、オンラインの要求があった場合のみ、暗号化してカード使用施設（店先）に送られてくる（会社キー）。埋込情報を復元するには双方のキーを突き合わせなければならない。

（c）カード所有者本人は、会社キーを、カード会社は、個人キーの内容を全く知らない。

【0032】

本カードシステムにおける本人の確認と正規カードであることの確認は、必要なレベル毎に以下の4つの手段がある。

（レベル1）目視による本人とカード上の顔写真の照合（盗んだり、拾ったりしたカードの不正使用の防止）

（レベル2）カード使用者に「パスワード」の入力を求め、ディスプレイに読み出された写真データとカードの顔写真との目視照合（カード顔写真の偽造防止）

（レベル3）カード所持者に「個人キー」の入力を求め、オンラインで送られてきた「会社キー」とつなぎ合わせ、写真データの中から、BPCS-Steg

anography技術によって埋め込まれていた個人情報を読み出せるかどうかを確認（カードがそっくり偽造されることの防止）

（レベル4）埋め込み個人情報（例えば指紋）によりカード所有者と使用者との照合（本来の所有者が、カードを他人に貸し与えることの防止）

【0033】

ここで、上記BPCS-Steganographyによる情報の埋込、抽出について、以下説明する。

すなわち、自然画像のビットプレーンでは、ノイズ状の領域を、別のノイズ状のデータに置き換えても、視覚的にほとんど影響を受けない。このことを利用すると、自然画像中のノイズ状の領域を秘密データで置き換えることが可能となる。ノイズ状の領域であるか否かの判定基準は、自然画像により異なるので、それぞれに適した閾値を求める必要がある。

2値画像において、 $2^m \times 2^m$ （通常は $m=3$ ）を局所領域サイズとした場合、閾値 α_{TH} に対して、

$$\alpha_{TH} \leq \alpha$$

を満たす領域は秘密データの埋め込み場所となる。

秘密データファイルを自然画像に埋め込むには、まず、そのファイルを $2^m \times 2^m$ ビット毎に区切り（ $2^m \times 2^m$ 画素に対応）、それらの各ファイル小片を、順次自然画像上の $2^m \times 2^m$ のノイズ状の領域に埋めていけばよい。しかしながら、すべてのファイル小片が α_{TH} より大きい複雑さを持つわけではない。そこで、そのような小片については、次で述べるコンジュゲーション演算により複雑化する。このような操作をすれば、どんな秘密ファイルも画像に埋め込むことが可能となる。ただしこの場合は、秘密ファイルを完全に復元するために、画像のどの領域がコンジュゲーションされたデータであるかを記録する“コンジュゲーション_マップ”を保存しておかなければならない。

以下、白画素の値を0、黒画素の値を1として考える。まず、Pを任意の2値画像とする。この時の背景は白とする。W、Bをそれぞれ、すべての画素が白、すべての画素が黒であるパターンと定義する。更に、2つの市松模様を W_C と B_C とする。ここで、 W_C は一番左上の画素が白であり、 B_C は逆に黒である（図

7参照)。Pは前景がBで、背景がWである画像だと見なされる。以上のことを前提として、Pの“コンジュゲート画像” P^* を以下のように定義する。

$$P^* = P \oplus W_c$$

ただし、 \oplus は各画素毎に排他的論理和演算を行うことを意味する。コンジュゲート画像を得る操作をコンジュゲーション演算と呼ぶこととする。この P^* は以下のような画像であると考えることができる。

- (1) 前景の形状はPと同様である。
- (2) 前景領域は B_C パターンである。
- (3) 背景領域は W_C パターンである。

このようなPと P^* は一対一に対応する。Pと P^* には以下のような性質がある。ただし、“ $\alpha(P)$ ”はPの複雑さ α を示す。

- (a) $(P^*)^* = P$
- (b) $P^* \neq P$
- (c) $\alpha(P^*) = 1 - \alpha(P)$

ここで最も重要な性質は(c)である。この性質は、簡単な画像を形状情報を失うことなく複雑な画像に変換(又はその逆)できることを示している。また、(a)により完全に元に戻すことも可能である。

本願で提案するステガノグラフィは以下の5つのステップからなる。

Step 1

$2^M \times 2^M$, $N_bits/pixel$ の自然画像をNビットのグレイコードに変換する。これは、河口英二などの、ビットプレーン分解して得られる2値画像とその複雑さに関する考察に基づいている。

Step 2

Step 1により生成されたグレイコード画像をビットプレーン分解によりN枚の2値画像に分解する。

Step 3

それぞれの2値画像を $2^m \times 2^m$ の部分画像に分割する。このとき、部分画像を P_i ; $i = 1, 2, \dots, 4^{M-m}$ と表記する。n番目のビットプレーン画像は次のように表現できる。

$$I_n = \{P_1^n, P_2^n, \dots, P_{4^{M-m}}^n\}$$

同様に、 n 番目の”コンジュゲーション_マップ”も以下のように表現できる。

$$C_n = \{Q_1^n, Q_2^n, \dots, Q_{4^{M-m}}^n\}$$

但し、 $Q_1^n, Q_2^n, \dots, Q_{4^{M-m}}^n$ は”0”又は”1”の値をとるものとする。ここで、”1”はコンジュゲーション演算を適用した領域を、”0”はそうでない領域を意味する。

埋め込みデータ (E と表記) は、ヘッダー、本体、パッドの3つの部分からなる。ヘッダーは本体のデータサイズを表し、本体は埋め込む秘密のデータそのもの (例えば秘密画像) である。パッドは、埋め込むデータを $2^m \times 2^m$ に整形するためのつめものである。 E_j ($j=1, 2, \dots, J$) をサイズが $2^m \times 2^m$ ビットの E の部分ビット系列とする。その E_j を1ビットずつラスタ走査の要領で、 $2^m \times 2^m$ の正方領域に対応させると、 $2^m \times 2^m$ の2値画像が生成でき、それを $\text{makeS}(E_j)$ と表記する。

閾値を α_{TH} とすると、埋め込みアルゴリズムは以下のように表現できる。ここで、 C_n の中の各 Q はすべて ”0” に初期化しておく。

```
for (n=N, j=1; n ≥ 1 && j < J; n--) {
  for (i=1; i ≤ 4^{M-m} && j < J; i++) {
    if (α(P_i^n) ≥ α_{TH}) {
      if (α(makeS(E_j)) ≥ α_{TH})
        P_i^n = makeS(E_j)
      else {
        P_i^n = makeS(E_j) *
        Q_i^n = "1"
      }
    }
    j++;
  }
}
```

下位ビットは画像に与える影響が少ないので、この埋め込み処理をビットプレーンの最下位ビットから順次実行する。 $makeS(E_j)$ が簡単な領域、つまり、その領域の複雑さが閾値より小さい場合、 $makeS(E_j)$ にコンジュゲーション演算を作用させる。この場合、コンジュゲーションマップの Q_j に“1”をセットする。

Step 4

情報が埋め込まれたN枚の2値画像からNビットのグレイコードを復元する。

Step 5

Step 4のグレイコードからNビット自然2進コードを求めると秘密データを埋め込んだ画像データとなる。

【0034】

秘密データの復元はこのアルゴリズムを逆に実行すればよい。ただし、そのためには閾値 α_{TH} とコンジュゲーションマップの情報が不可欠である。

【0035】

以下、図2～図6を参照してICカードシステムとしてこの発明を適用した実施例を説明する。図2はICカードシステムの概念を示すブロック図である。図3はシステムのICカードおよびリーダライタの概略の構成を示すブロック図である。図4は同じくICカードの他の構成例を示すブロック図である。図5、図6はシステムで実行されるプログラムを示すフローチャートである。

これらの図に示すように、この発明に係る情報カードとしてのICカード100は、リーダライタ200（データ処理端末）との間でデータの授受が可能である。リーダライタ200は例えばクレジット会社などが管理するホストコンピュータ300との間でもオンラインによりデータの授受を可能としている。リーダライタ200は、ディスプレイ210（表示手段）、入力手段220（マウス、キーボードなど）を有して構成することもできる。

【0036】

図3に示すように、ICカードのリーダライタ200は、演算処理などを行うCPU、データを格納するデータメモリ、プログラムを格納するプログラムメモ

リ、バッファメモリ、データの入力などを行うキーボード、演算処理結果を表示する表示部、ICカードとの入出力を制御するためのインタフェース、電源部を有して構成されている。

このリーダライタ200は、ICカード100に対してデータの読み書きを行うことを可能としても良い。CPUは暗号化・復号化および認証処理等を実行し、プログラムメモリにはアプリケーションプログラム等が書き込まれている。

ICカード100は、インタフェース、CPU、プログラムメモリ、データメモリを有している。ICカード100への電源はリーダライタ200の電源部から供給される。

プログラムメモリ、データメモリは不揮発性メモリで構成され、この不揮発性メモリは、電氣的消去可能なEEPROM、あるいは、バッテリバックアップされたスタティックRAM等により構成されている。

また、図4はICカードの他の構成例である。すなわち、CPUが制御部、演算部、ROM、RAMを有し、PROMにデータを記憶し、コネクタ部によって外部装置（リーダライタ）と接続する構成である。

【0037】

このICカードはプラスチック板材にICチップを埋設して構成され、そのカード表面には、所有者名、カード番号、有効期限などがエンボス加工などで表示されている。

ICチップには、そのメモリ（8KB以上）に、パスワード情報、顔写真のデジタルデータまたは音響データ（情報データ）が記憶されているとともに、これらの情報データにはBPCS-Steganography技術による本人の個人情報（例えば指紋データ）、所有者の顔写真、個人情報の一部（デジタル署名画像）が埋め込まれて格納されている。

【0038】

このICカードシステムによれば、目視による利用者の確認と、機械的なカード認証が同時に可能である。そして、このICカードでは、その秘密の存在を気付かせない。また、秘密の存在に気付いても取り出せない。このICカードにデジタル情報や認証情報を隠しておき、その認証情報を正確に読み込み、埋め込み

が可能である。

【0039】

図5には、ステガノグラフィによるICカードへのデータの格納プロセス（エンコーダプログラム）を示す。まず、ICカードのメモリ（8KB以上）に書き込むための顔写真データ（インデックス付き顔写真データを含む）を作成する。これをビットマップファイルとして保存する。この場合、顔写真データの大きさはメモリの75%程度とする。また、この顔写真データとしては、ICカード所有者本人の顔写真データを使用する。

次に、この顔写真データに埋め込むための個人の認証情報（テキスト）を作成、保存する。このテキストデータは顔写真データの10%程度とする。

この顔写真データおよび認証情報を選択、表示する。

次に、このICカード用顔写真データを自然2進コード（PBC）に変換する。

次いで、変換後の顔写真データを正準グレイコード（CGC）に変換する。

さらに、変換後の顔写真データをビットプレーン分解する（N枚の2値画像に分解する）。このビットプレーン分解後の顔写真データに上記個人の認証情報（テキストデータ）を埋め込む。埋込方法としては、カスタマイズキー（たとえば24桁のデータとする）を用いて上述のアルゴリズムにより個人の認証情報を埋め込むものとする。

そして、この顔写真データを自然2進コード（PBC）に変換する。

さらに、ICカード用の顔写真データを作成し、保存する。

ここで、リーダライタにICカードを挿入し、任意に顔写真データを選択し、これをICカードのメモリに転送、保存する。そして、この顔写真データの保護用にパスワードをICカードのメモリに設定、保存する。パスワードは例えば4桁のデータとする。

以上の結果、ICカード（例えば身分証明用カード）が作成される。この後、ICカードのプラスチック板表面に所有者個人の写真などが印刷されることとなる。

【0040】

次に、図6を参照してICカードの認証について説明する。図6はデコーダプログラムの一部を示す。

まず、ICカードをリーダライタに挿入する。すると、リーダライタでは認証フローを実行するためのイニシャライズが実行される。次に、キーボードなどによってパスワードの入力が行われる。そして、この入力されたパスワードを、リーダライタが、ICカードのメモリに記憶保持するパスワードと照合する。一致しておれば、ICカードのメモリに保持された顔写真データ（情報データ）を読み出し、ディスプレイに表示する。この顔写真データが所有者本人の顔写真を示す場合、これとカード本体表面に貼り付けられた写真との照合、表示画像と本人との照合がそれぞれ目視によりなされる。

次いで、カスタマイズキーが入力される。このカスタマイズキーは上記個人認証情報の埋込に使用されたもので、所有者本人のみが知るキーである。このカスタマイズキーはICカードのメモリに格納されておらず、上記固有データの埋込と抽出とを制御するパラメータである。したがって、固有データの抽出のために入力されたカスタマイズキーが、埋込に用いられたパラメータと一致するときのみ、固有データが情報データより抽出されることとなる。

具体的には、ICカードのメモリより読み出した顔写真データ（情報データ）について自然2進コード（PBC）に変換する。次いで、この変換後の顔写真データをグレイコード（CGC）に変換する。さらに、この顔写真データはビットプレーン分解される。ここで、カスタマイズキーを用いてこのビットプレーン分解後の顔写真データより、個人の認証情報が取り出される。このようにして、顔写真データより個人の認証情報（テキストデータ）が抽出され、表示される。

なお、パスワードが一致しない場合はICカードのメモリから顔写真データを読み出すことができず、また、カスタマイズキーが一致しない場合は、顔写真データから認証情報を抽出することができない。そして、これらの不一致の場合、そのICカードは偽造または不正使用に係るものとして、リーダライタから排出、回収などされる。

【0041】

以上の結果、このICカードシステムにあっては、目視より所有者本人の使用

か否かを確認した後、パスワード照合で顔写真データの読み出しおよび顔写真データに基づく顔写真画像の表示を許可する。そして、この表示した顔写真画像を貼付写真と比較することで、さらにＩＣカードの正当性がチェックされる。そして、カスタマイズキーを用いて、この顔写真データから個人情報を抽出し、表示する。この表示された個人情報を、本人のそれと比較することにより、真正なカードであることを確認する。

このように、見かけ上の画像データの中に、別の画像データ、音声データ、テキストデータが同時に潜んでおり、これをチェックすることにより、本人による真正カードの使用であることを確認することができる。

【0042】

【発明の効果】

請求項１に記載の発明では、秘密情報である固有データの存在を第三者に気付かれることがないため、情報カードのセキュリティを高めることができる。

【0043】

請求項２に記載の発明では、固有データにより情報カードの正当性を検証することができる。正当性データ、所有者データの存在を隠すことができる。

【0044】

請求項３に記載の発明では、パスワードにより情報データを保護することができる。カードのセキュリティを高めることができる。

【0045】

請求項４に記載の発明では、カスタマイズキーによって、固有データの保護を図ることができる。

【0046】

請求項５に記載の発明では、パスワードの照合により、情報データの読み出しを保護することができる。

【0047】

請求項６に記載の発明では、無権限者による固有データの抽出を防止することができ、高度のセキュリティを与えることができる。

【0048】

請求項 7 に記載の発明では、パスワードおよびカスタマイズキーによって情報カードの不正使用を防止することができる。

【0049】

請求項 8 に記載の発明では、3 重のセキュリティを施すことができ、情報カードの偽造、不正使用を完全に排除することができる。

【0050】

請求項 9 に記載の発明では、固有データはステガノグラフィにより埋め込まれるため、その解読が困難で、秘匿性が高い。

【0051】

請求項 10 に記載の発明では、固有データに各種ファイルを埋め込むことが可能である。

【0052】

請求項 11 に記載の発明では、メモリカードまたは IC カードとして情報カードおよびそのシステムを構成可能である。リーダライタを安価に設けることも可能となる。

【0053】

請求項 12 に記載の発明では、写真と画像データとの照合が可能となる。写真の偽造を防止することができる。

【図面の簡単な説明】

【図 1】

この発明に係る情報カードシステムの機能構成を示すブロック図である。

【図 2】

この発明の一実施例に係る情報カードシステムを表すブロック図である。

【図 3】

この発明の一実施例に係る情報カードシステムの電氣的構成を示すブロック図である。

【図 4】

この発明の一実施例に係る情報カードの電氣的構成を示すそのブロック図である。

【図 5】

この発明の一実施例に係る情報カードシステムでの埋込手順（エンコードプログラム）を表すフローチャートである。

【図 6】

この発明の一実施例に係る情報カードシステムでの認証手順（デコードプログラム）を表すフローチャートである。

【図 7】

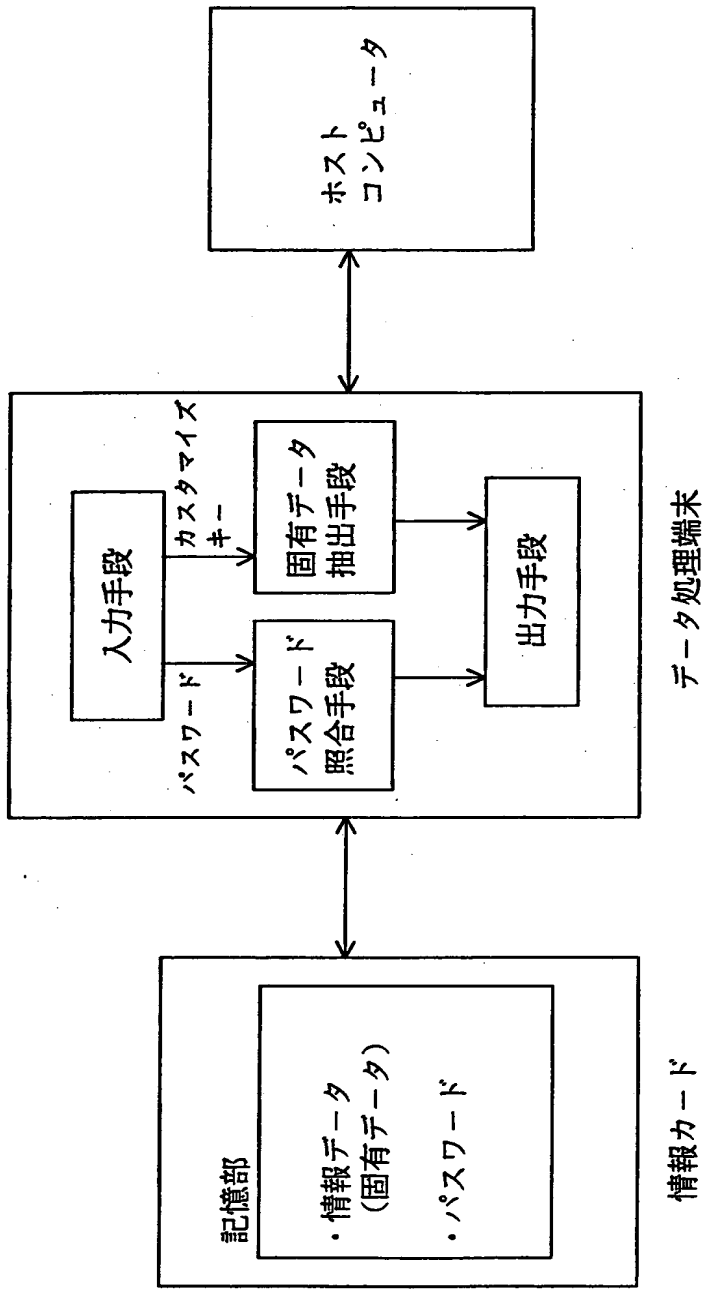
この発明に係るコンジュゲーション演算を説明するための模式図である。

【符号の説明】

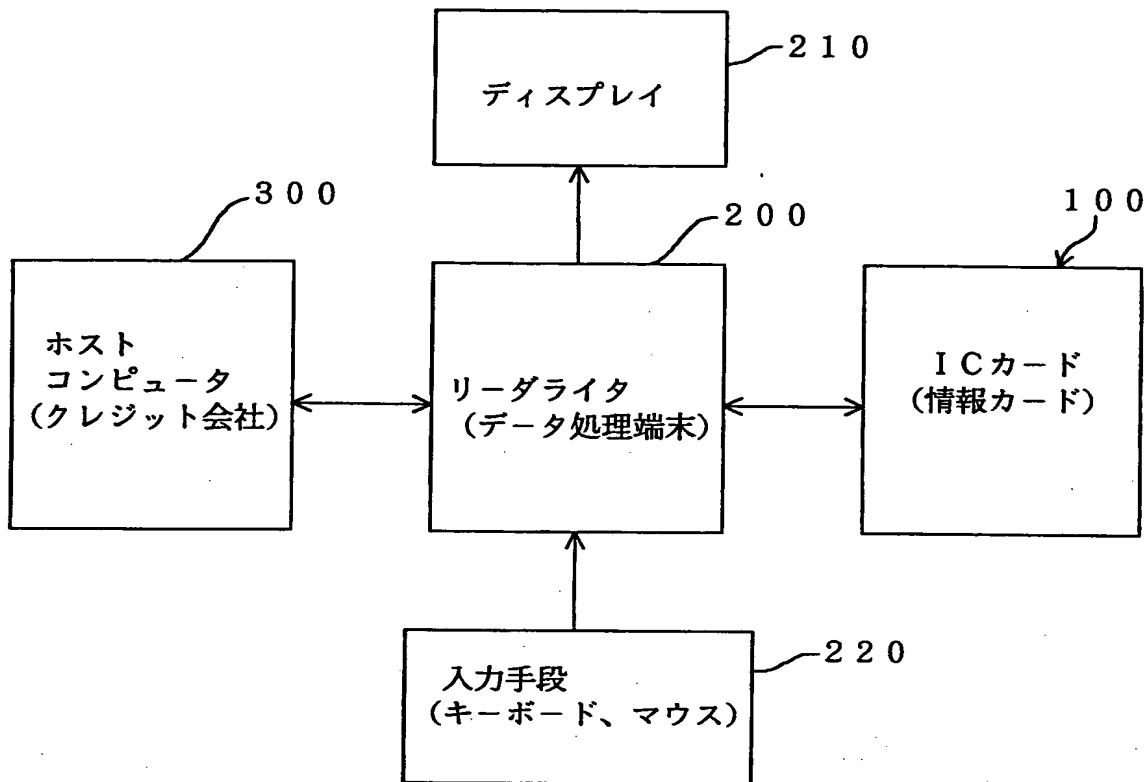
- 100 ICカード（情報カード）、
- 200 リーダライタ（データ処理端末）、
- 300 ホストコンピュータ。

【書類名】 図面

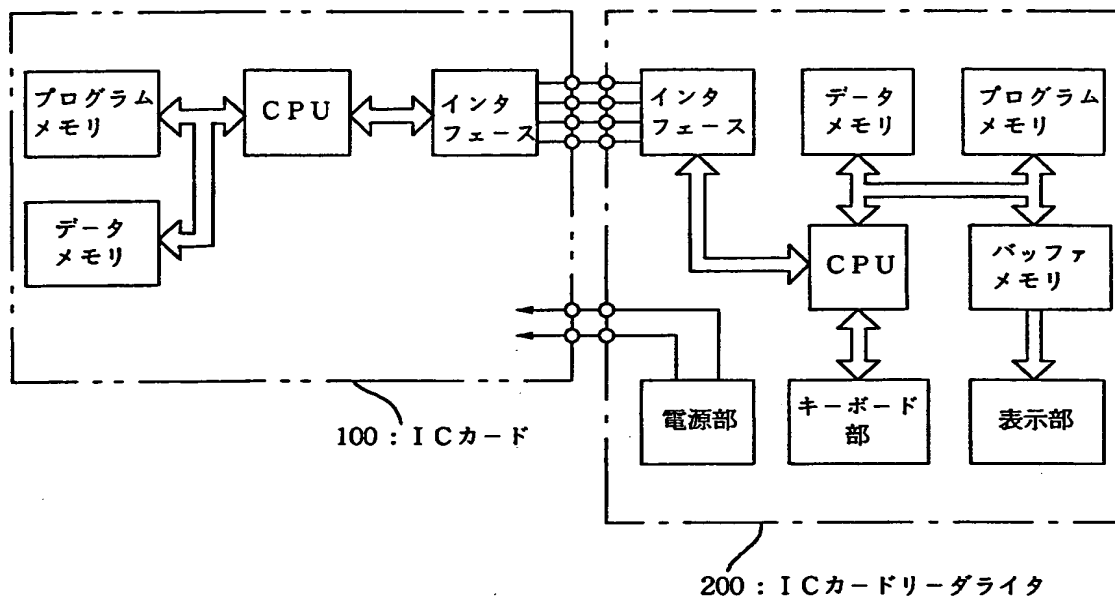
【図 1】



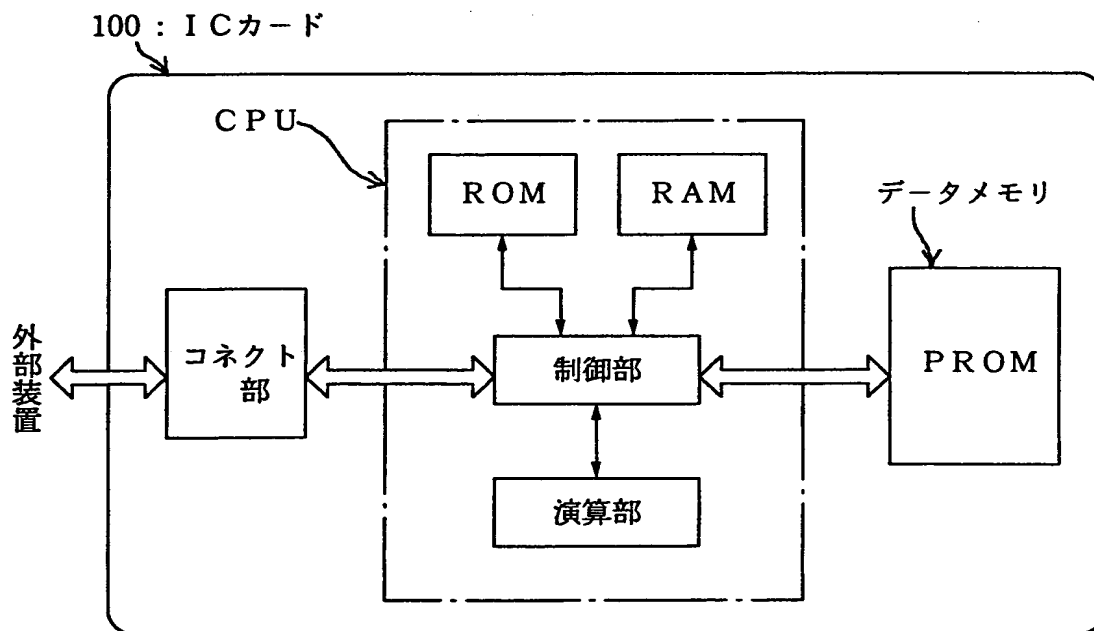
【図 2】



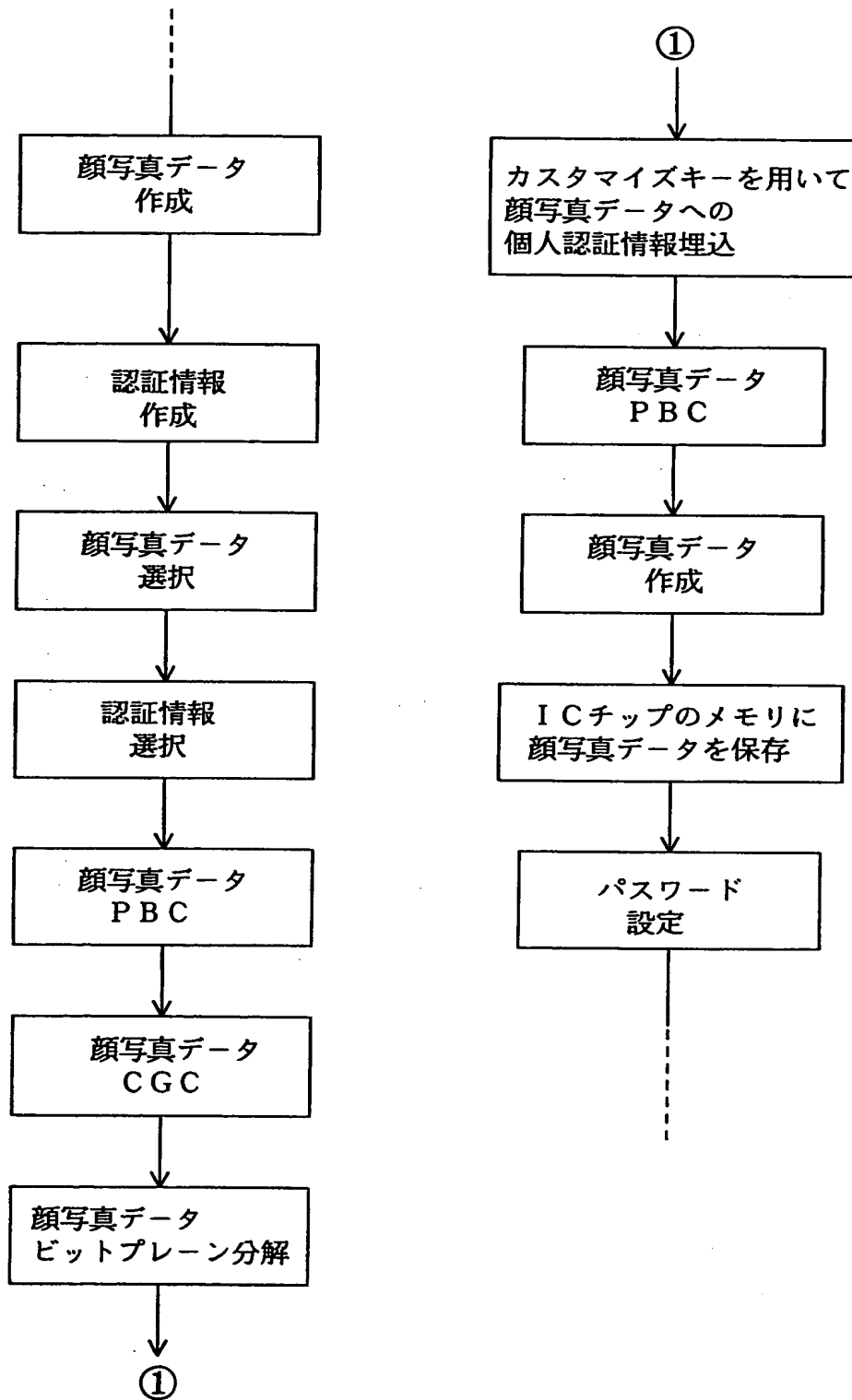
【図 3】



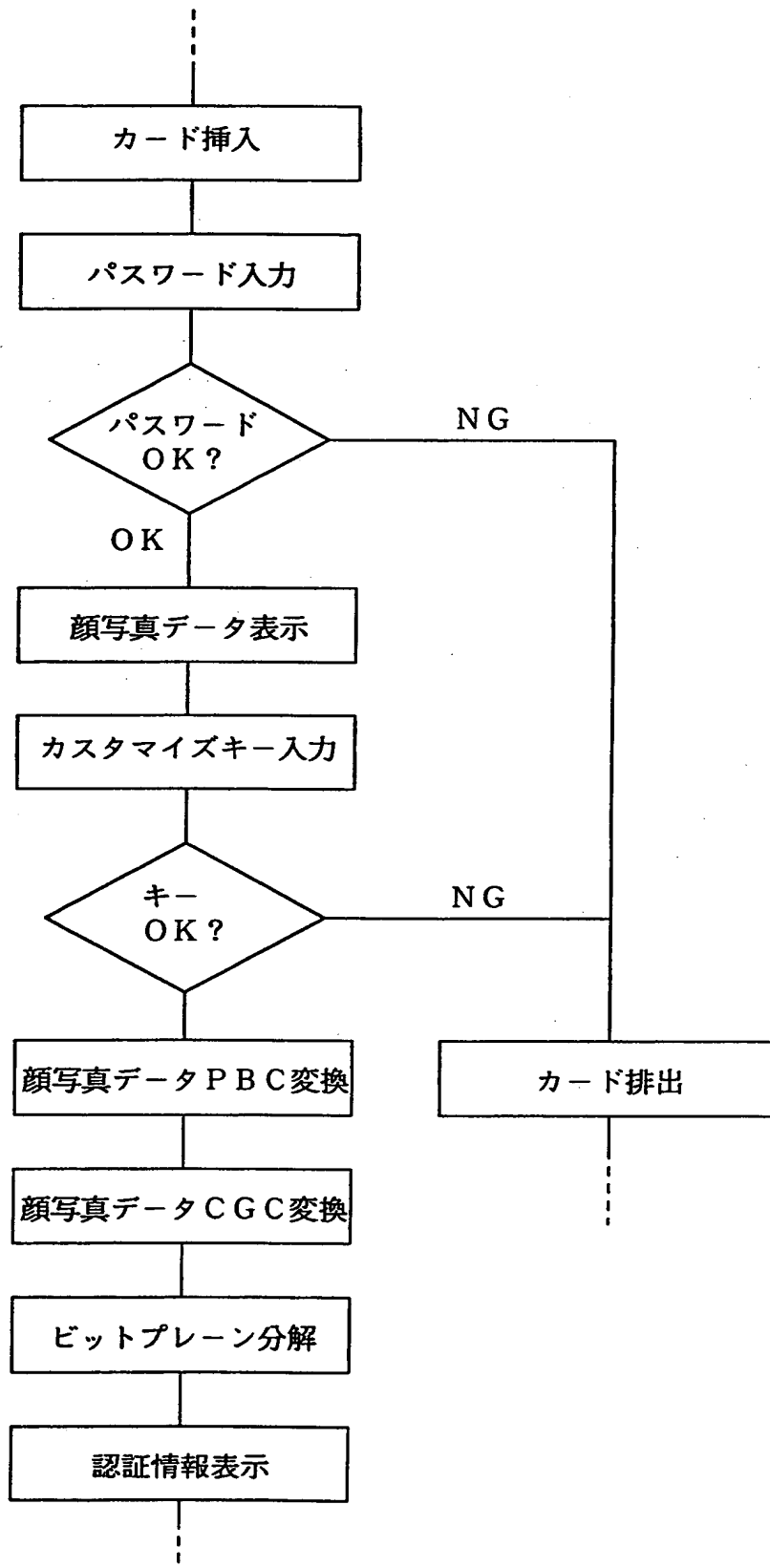
【図 4】



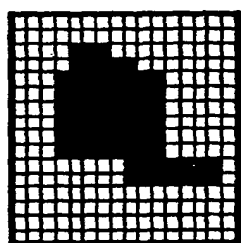
【図 5】



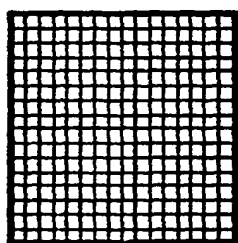
【図 6】



【図 7】



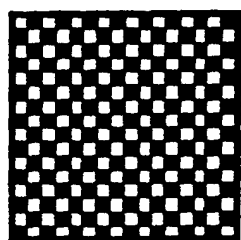
(A) P



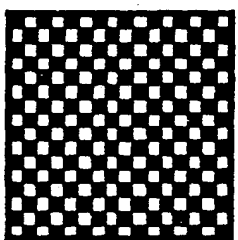
(B) W



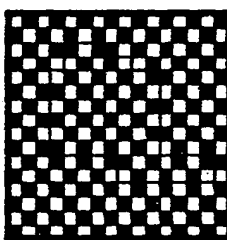
(C) B



(D) W_c



(E) B_c



(F) P^*

【書類名】 要約書

【要約】

【目的】 カードの偽造、不正使用を完全に排除した情報カードシステムを提案する。

【構成】 情報カードの記憶部に情報データを格納し、この情報データにステガノグラフィによる固有データを埋め込む。情報データの読み出しを許可するためのパスワードも情報カードに格納する。データ処理端末は、入力されたパスワードを格納したパスワードと照合し、一致したとき、情報データの読み出しを許可する。また、入力されたカスタマイズキーを用いて固有データを抽出する。正規のカスタマイズキーの場合に限り、固有データの抽出が許容される。このシステムでは、固有データの存在を秘匿することができ、かつ、その抽出を防止することができる。無権限者はカスタマイズキーを知ることができないからである。よって、システム自体のセキュリティが高められている。

【選択図】 図1

【書類名】 職権訂正データ
【訂正書類】 特許願

<認定情報・付加情報>

【特許出願人】

【識別番号】 598132923
【住所又は居所】 福岡県北九州市戸畑区中原新町3-3
【氏名又は名称】 株式会社エーエスエー・システムズ

【特許出願人】

【識別番号】 598132934
【住所又は居所】 福岡県宗像市日の里8丁目21番地の2
【氏名又は名称】 河口 英二

【特許出願人】

【識別番号】 598132945
【住所又は居所】 アメリカ合衆国 04473 メイン州 オロノ市
アールアール5 ボックス240ケイ
【氏名又は名称】 リチャード オー イースン

【代理人】

申請人
【識別番号】 100094215
【住所又は居所】 福岡県北九州市小倉北区京町3丁目14番8-80
A号 協栄小倉ビル
【氏名又は名称】 安倍 逸郎

出 願 人 履 歴 情 報

識別番号 [598132923]

1. 変更年月日 1998年 9月29日

[変更理由] 新規登録

住 所 福岡県北九州市戸畑区中原新町3-3

氏 名 株式会社エーエスエー・システムズ

出 願 人 履 歴 情 報

識別番号 [598132934]

1. 変更年月日	1998年 9月29日
[変更理由]	新規登録
住 所	福岡県宗像市日の里8丁目21番地の2
氏 名	河口 英二

出 願 人 履 歴 情 報

識別番号 [598132945]

1. 変更年月日 1998年 9月29日

[変更理由] 新規登録

住 所 アメリカ合衆国 04473 メイン州 オロノ市 アールア
ール5 ボックス240ケイ

氏 名 リチャード オー イースン

